Removable media

INFOSEC

What is removable media?

Removable media is any device that can be hooked up to a computer and used to store or transfer files or information. This can be a USB drive, a smartphone, an external hard drive and more. They can also be dangerous.

Seriously? A USB drive can be dangerous?

Attackers may drop infected removable media for other people to find and plug in, spreading the malware. Never open or plug in any removable media devices you find!

Why would someone pick up a dropped drive?

Most of the time, they're just being good people. A recent test with 297 dropped drives on a university campus found that 98% of the drives were picked up. Of the people who picked up the drives, 68% did so with the intention of using the drive's files to locate the owner.

How would someone bait you into picking up removable media?

An attacker might try to make the bait more attractive. Writing something like "confidential" or "new salary info" on the drive or disk will make it hard for people to resist picking it up.

So what do I do if I find a USB drive lying around?

Follow your organization's policies for found media. Most organizations will want any found media turned in to the IT department or the security desk for safe disposal.

What are good tips for using removable media safely?

Use encrypted media. Encrypt your phone, your drives and any other removable media you use. This will keep it safe if it's lost or stolen. Second, be careful what you store on removable media. Be sure to check your organization's policies on what can be stored and where.

Sources: https://elie.net/static/files/users-really-do-plug-in-usb-drives-they-find/users-really-do-plug-in-usb-drives-they-find-paper.pdf